Amendments to the Drawings:

The attached sheet of drawings includes changes to Fig. 25. This sheet replaces the original sheet.

Attachment: Replacement Sheet

REMARKS

This Amendment is in response to the Office Action mailed March 12, 2007. Applicant respectfully traverses the rejections in their entirety. On June 6, 2007, the undersigned attorney conducted a telephone conference and discussed the allowability of the claims, in particular the independent claims. The particulars of the telephone conference are outlined in our request to withdraw the rejections are described below.

Drawings

A particular drawing (FIG. 25) was objected to because it allegedly failed to illustrate a second cryptographic unit (1160). Applicant respectfully disagrees because CP decryption/encryption logic 1550/1560 is part of the second cryptographic unit. However, to clarify the invention, FIG. 25 has been amended to include an illustration of the second cryptographic unit (1160) and respectfully requests that the Examiner withdraw this outstanding objection.

Rejection Under 35 U.S.C. § 102

Claims 1-4, 6, 8, 10-13, 18-19, 22, 28 and 29 were rejected under 35 U.S.C. §102(b) as being anticipated by Wasilewski (U.S. Patent Publication No. 2002/0094084). Applicant respectfully requests the Examiner to withdraw this rejection because a *prima facie* case of anticipation has not been established.

As the Examiner is aware, to anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Vergegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the...claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989). Herein, all of the claim limitations are not found in Wasilewski.

For instance, with respect to claim 1, the Office Action alleges that Wasilewski describes that the concatenation of the multi-session key (MSK), control word and other data constitutes the "first value generated based on a conditional access (CA) random value and the unique key",

the MAC as the second value, and the clear control word (CW) as the third value. *See Page 3 of the Office Action.* Applicant disagrees with this interpretation, but even assuming this interpretation is accurate, Applicant respectfully points out that the third value (clear CW) is not recovered by a cryptographic operation (e.g., decryption or other cryptographic recovery technique) using the second value (MAC). Rather, the clear CW is recovered using the MSK. The MAC is exclusively used as a comparison value with a hash value of the recovered clear CW in order to authenticate the recovered clear CW before releasing for use in decryption operations.

Similarly, Applicant respectfully submits that the 102(b) rejection as applied to claim 13 is also improper. Claim 13 includes the limitation that the control word recovered *by decrypting an encrypted control word using the second value. Emphasis added.* Wasilewski clearly illustrates that the MSK, namely a portion of the first value as interpreted, enables "recovery" of the clear CW (third value). Again, the MAC (second value) has no involvement in the recovery of the third value as claimed.

Therefore, Applicant respectfully requests withdrawal of the outstanding §102(b) rejection as applied to claims 1 and 13.

With respect to claim 22, as discussed with the Examiner, the Office Action alleges that Wasilewski describes the "first process block" being logic that produces the "first derivative key" (the concatenation of the MSK, control word and other data). Moreover, the Office Action alleges that Wasilewski describes the second process block that is configured to generate a mating key (MAC) from a mating key generator (hash function) using the first key (concatenation of the MSK, control word and other data) and the third process block is configured to recover the control word (CW) by decrypting an encrypted control word using the mating key. *See Page 4 of the Office Action.* Applicant disagrees with this interpretation, but even assuming this interpretation is accurate, Applicant respectfully points out that the CW is not recovered by an encrypted control word (encrypted CW) using the mating key (MAC). Rather, the CW is recovered using the MSK.

Therefore, Applicant respectfully requests withdrawal of the outstanding §102(b) rejection as applied to claim 22.

With respect to claim 28, similar to the arguments presented above, Wasilewski does not describe the recovery of the plurality of control words using the plurality of mating keys. Applicant incorporates the arguments made above and respectfully requests the Examiner to withdraw the rejection or to provide ample evidence in support of the rejection. Withdrawal of the outstanding §102(b) rejection is respectfully requested.

With respect to claims 2-4, 6, 8, 10-12, 18-19 and 29, Applicant respectfully traverses the outstanding §102(b) rejection because a *prima facie* case of anticipation has not been established for these claims. Based on the dependency of the above-identified claims on independent claims 1, 13 and 28, which are believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traversing the rejection is necessary. For illustrative purposes, however, we shall discuss a few of these claims to illustrate that Wasilewski clearly does not anticipate these claims.

For instance, with respect to claims 2, 14, and 23, the Examiner states that Wasilewski discloses descrambler of claim 1 being a single integrated circuit. However, Wasilewski describes the descrambler operations, which are collectively performed with a Service Access Broadband Encryption Remapper (SABER) and a set-top unit (STU). These devices are clearly positioned in separate physical locations and, upon review, the implementation of claimed operations by the SABER and STU within a single integrated circuit is unreasonable and contrary to the teachings of Wasilewski.

Moreover, with respect to claim 4, for example, the Examiner states that Wasilewski discloses that the first value is a derivative key generated by performing a decryption operation on the CA random value using the unique key. We disagree. As construed in claim 1, the first value is considered by the Examiner to be the collection of the "multi-session key (MSK), control word and other data". This value is not a derivative key that is generated by performing a decryption operation on the "other data" that is considered by the Examiner to be the CA random value.

Applicant respectfully requests outstanding §102(b) rejection as applied to claims 2-4, 6, 8, 10-12, and 18-19 and 29 be withdrawn. Applicant reserves the right to present additional arguments if an Appeal is warranted.

Rejection Under 35 U.S.C. § 103

Claims 5, 7, 9, 20-21 and 26-27 were rejected under 35 U.S.C. §103(a) as being unpatentable over Wasilewski. Furthermore, claims 15-17, 24-25, and 30-32 were rejected under 35 U.S.C. §103(a) as being unpatentable over Wasilewski in view of Wasilewski (U.S. Patent Publication No. 2004/003008), hereinafter referred to as "Wasilewski '008".

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988).*

Herein, neither Wasilewski nor Wasilewski '008, alone or in combination, describe or suggest all of the claim limitations set forth in these claims, especially those limitations denoted above in traversing the outstanding §102(b) rejection. Applicant incorporates these arguments by reference. Also, based on the dependency of the above-identified claims on independent claims 1 and 13 and 22, which are believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traversing the rejection is necessary.

Applicant respectfully requests that the Examiner withdraw the rejection of claims 5, 7, 9, 15-17, 20-21 and 24-27 and 30-32 under 35 U.S.C. § 103(a) as being unpatentable over Wasilewski and/or Wasilewski '008.

Conclusion

Applicant reserves all rights with respect to the applicability of the doctrine of equivalents. Applicant respectfully requests that a timely Notice of Allowance be issued in this case.